PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : H04L 9/30 | A1

(11) Internationale Veröffentlichungsnummer: **WO 99/43124**

(43) Internationales Veröffentlichungsdatum: 26. August 1999 (26.08.99)

(21) Internationales Aktenzeichen: PCT/DE99/00278

(22) Internationales Anmeldedatum: 2. Februar 1999 (02.02.99)

(30) Prioritätsdaten:
198 06 825.5 18. Februar 1998 (18.02.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: HESS, Erwin [DE/DE]; Gottfried–Keller–Strasse 36, D–85521 Ottobrunn (DE). GEORGIADES, Jean [GR/DE]; Ungererstrasse 68 A, D–80805 München (DE).

(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, D–80506 München (DE).

(81) Bestimmungsstaaten: BR, CA, CN, IN, JP, KR, MX, RU, UA, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: ELLIPTIC CURVE CRYPTOGRAPHIC PROCESS AND DEVICE FOR A COMPUTER

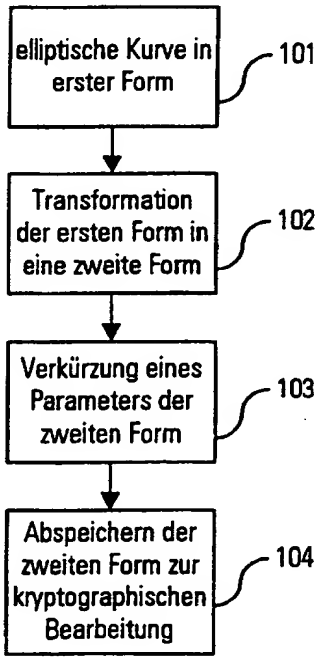
(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR KRYPTOGRAPHISCHEN BEARBEITUNG ANHAND EINER ELLIPTISCHEN KURVE AUF EINEM RECHNER

(57) Abstract

In elliptic curve cryptographic processing, the elliptic curve parameters are stored in the memory of a computer. These parameters are considerably long. In order to reduce the length of at least one parameter while maintaining a high degree of security, the elliptic curve is transformed. A parameter is shortened, preferably to 1, –1, 2 or –2, while the other parameters are several hundred bits long. Precisely in the case of chip cards, which have little storage space, even a single shortened parameter can already have a distinct effect.

(57) Zusammenfassung

Bei der kryptographischen Bearbeitung anhand einer elliptischen Kurve werden Parameter der elliptischen Kurve in einem Speicher eines Rechners abgespeichert. Diese Parameter weisen jeweils erhebliche Länge auf. Um mindestens einen Parameter in seiner Länge deutlich zu verkürzen und dabei unverändert hohe Sicherheit zu gewährleisten, wird die elliptische Kurve transformiert. Mit einem Algorithmus wird ein Parameter bevorzugt zu 1, –1, 2 oder –2 verkürzt, wohingegen die anderen Parameter mehrere 100–Bit Länge aufweisen. Gerade bei Chipkarten, die wenig Speicherplatz aufweisen, macht sich die Verkürzung schon eines Parameters deutlich bemerkbar.



101 ... ELLIPTIC CURVE IN A FIRST SHAPE
102 ... TRANSFORMATION OF THE FIRST SHAPE INTO A SECOND SHAPE
103 ... REDUCTION OF A PARAMETER OF THE SECOND SHAPE
104 ... STORING THE SECOND SHAPE FOR CRYPTOGRAPHIC PROCESSING

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Beschreibung

Verfahren und Vorrichtung zur kryptographischen Bearbeitung anhand einer elliptischen Kurve auf einem Rechner

Die Erfindung betrifft ein Verfahren und eine Anordnung zur kryptographischen Bearbeitung anhand einer elliptischen Kurve auf einem Rechner.

Ein endlicher Körper heißt Galois-Feld. Zu den Eigenschaften und zur Definition des Galois-Feldes sei auf [3] verwiesen.

Mit der weiten Verbreitung von Computernetzen und zugehörigen Anwendungen, die über elektronische Kommunikationssysteme (Kommunikationsnetze) abgewickelt werden, werden zunehmend wachsende Anforderungen an die Datensicherheit gestellt. Der Aspekt der Datensicherheit berücksichtigt u.a.

- die Möglichkeit eines Ausfalls der Datenübertragung,
- die Möglichkeit korrumpierter Daten,
- die Authentizität der Daten, also die Feststellbarkeit und die Identifikation eines Absenders und
- den Schutz der Vertraulichkeit der Daten.

Unter einem "Schlüssel" werden Daten verstanden, die bei der kryptographischen Bearbeitung Verwendung finden. Aus Public-Key-Verfahren [4] ist bekannt, einen geheimen und einen öffentlichen Schlüssel einzusetzen.

Ein "Angreifer" ist eine nichtautorisierte Person mit dem Ziel, an den Schlüssel zu gelangen.

Insbesondere in einem Rechnernetz, in zunehmenden Maße aber auch in portablen Medien, z.B. einem Mobiltelefon oder einer Chipkarte, ist sicherzustellen, daß ein abgespeicherter Schlüssel auch dann nicht zugänglich ist, wenn ein Angreifer sich des Rechners, des Mobiltelefons oder der Chipkarte bemächtigt.

Um ausreichende Sicherheit kryptographischer Verfahren zu gewährleisten, werden Schlüssel, insbesondere bei asymmetrischen Verfahren, jeweils mit Längen von mehreren 100 Bits bestimmt. Ein Speicherbereich eines Rechners oder portablen Mediums ist zumeist knapp bemessen. Eine Länge eines in einem solchen Speicherbereich abgelegten Schlüssels von mehreren 100 Bits verringert den freien Speicherplatz auf dem Rechner bzw. dem Medium, so daß nur wenige solcher Schlüssel auf einmal abgespeichert werden können.

Aus [1] und [2] ist eine elliptische Kurve und deren Anwendung bei der kryptographischen Bearbeitung bekannt.

Die **Aufgabe** der Erfindung besteht darin, ein Verfahren zur kryptographischen Bearbeitung anhand mindestens einer elliptischen Kurve auf einem Rechner anzugeben, wobei weniger Speicherplatz benötigt wird.

Diese Aufgabe wird gemäß der Merkmale der unabhängigen Patentansprüche gelöst.

Es wird ein Verfahren zur kryptographischen Bearbeitung anhand mindestens einer elliptischen Kurve auf einem Rechner angegeben, bei dem die elliptische Kurve in einer ersten Form vorgegeben wird, wobei mehrere erste Parameter die elliptische Kurve in der ersten Form bestimmen. Die elliptische Kurve wird in eine zweite Form transformiert, indem mehrere zweite Parameter bestimmt werden, wobei mindestens einer der zweiten Parameter in seiner Länge gegenüber einem der ersten Parameter verkürzt wird. Die elliptische Kurve nach der Transformation, also in der zweiten Form, wird zur kryptographischen Bearbeitung verwendet.

Durch die signifikante Verkürzung eines der ersten Parameter ergibt sich eine Einsparung eines für diesen Parameter

bereitzustellenden Speicherbereichs. Da der Speicherbereich, z.B. auf einer Chipkarte, eng bemessen ist, erreicht man durch die Einsparung mehrerer 100 Bit für jeden verkürzten Parameter freien Speicherplatz z.B. zum Abspeichern eines weiteren geheimen Schlüssels. Durch die Verkürzung des jeweiligen Parameters bleibt ist die Sicherheit des kryptographischen Verfahrens trotzdem gewährleistet.

Bei Verwendung einer elliptischen Kurve in einem kryptographischen Verfahren steigt der Aufwand für einen Angreifer, den Schlüssel zu ermitteln, exponentiell mit dessen Länge.

Eine Weiterbildung der Erfindung besteht darin, daß die erste Form der elliptischen Kurve bestimmt ist durch:

$$y^2 = x^3 + ax + b \text{ über } GF(p) \qquad (1)$$

wobei

GF(p) ein Galois-Feld mit p Elementen und

x,y,a,b Elemente des Körpers GF(p)

bezeichnen.

Die später verwendete Bezeichnung "mod p" bezeichnet einen Spezialfall für das Galois-Feld, nämlich die natürlichen Zahlen kleiner p. "mod" steht für MODULO und umfaßt eine Ganzzahldivision mit Rest.

Eine andere Weiterbildung besteht darin, daß die zweite Form der elliptischen Kurve bestimmt ist durch

$$y^2 = x^3 + c^4ax + c^6b \text{ über } GF(p) \qquad (2)$$

wobei c eine Konstante bezeichnet.

Zur Einsparung von Speicherplatz wird Gleichung (1) in Gleichung (2) transformiert und eine die elliptische Kurve gemäß Gleichung (2) kennzeichnende Größe verkürzt.

Eine Weiterbildung besteht darin, den Parameter a zu verkürzen, indem die Konstante c derart gewählt wird, daß

$$c^4 a \bmod p \qquad (3)$$

deutlich kürzer wird als die anderen die elliptische Kurven nach Gleichung (2) beschreibenden Parameter. Durch diese Verkürzung benötigt der Parameter entsprechend weniger Speicherplatz.

Auch ist es eine Weiterbildung, das Verfahren in einer der folgenden Anwendungen einzusetzen:

- Verschlüsselung bzw. Entschlüsselung:
  Daten werden von einem Sender verschlüsselt - mittels symmetrischem oder asymmetrischem Verfahren - und auf der Gegenseite bei einem Empfänger entschlüsselt.
- Schlüsselvergabe durch eine Zertifizierungsinstanz:
  Eine vertrauenswürdige Einrichtung (Zertifizierungsinstanz) vergibt den Schlüssel, wobei sichergestellt werden muß, daß der Schlüssel von dieser Zertifizierungsinstanz stammt.
- digitale Signatur bzw. Verifikation der digitalen Signatur:
  Ein elektronisches Dokument wird signiert und die Signatur dem Dokument angefügt. Bei dem Empfänger kann anhand er Signatur festgestellt werden, ob auch wirklich der gewünschte Sender unterschrieben hat.
- asymmetrische Authentikation:
  Anhand eines asymmetrischen Verfahrens kann ein Benutzer seine Identität nachweisen. Vorzugweise geschieht das durch Codierung mit einem entsprechenden geheimen (privaten) Schlüssel. Mit dem zugehörigen öffentlichen Schlüssel dieses Benutzers kann jeder feststellen, daß die Codierung wirklich von diesem Benutzer stammt.

- Verkürzen von Schlüsseln:
  Eine Variante der kryptographischen Bearbeitung umfaßt das Verkürzen eines Schlüssels, welcher Schlüssel bevorzugt für weitergehende Verfahren der Kryptographie verwendet werden kann.

Ferner ist eine Vorrichtung angegeben, die eine Prozessoreinheit aufweist, die derart eingerichtet ist, daß eine elliptische Kurve in einer ersten Form vorgegeben wird, wobei mehrere erste Parameter die elliptische Kurve bestimmen, und daß die elliptische Kurve in eine zweite Form transformiert wird, indem mehrere zweite Parameter bestimmt werden, wobei mindestens einer der zweiten Parameter in seiner Länge gegenüber den ersten Parameter verkürzt wird. Schließlich wird die elliptische Kurve in der zweiten Form zur kryptographischen Bearbeitung bestimmt.

Diese Vorrichtung kann eine Chipkarte sein, die einen geschützten und einen nicht geschützten Speicherbereich aufweist, wobei sowohl in dem geschützten als auch in dem nichtgeschützten Speicherbereich Schlüssel, also Parameter, die die elliptische Kurve kennzeichnen, abgelegt werden können.

Diese Vorrichtung ist insbesondere geeignet zur Durchführung des erfindungsgemäßen Verfahrens oder einer seiner vorstehend erläuterten Weiterbildungen.

Weiterbildungen der Erfindung ergeben sich auch aus den abhängigen Ansprüchen.

Anhand der folgenden Figur werden Ausführungsbeispiele der Erfindung näher dargestellt.

Es zeigen

Fig.1 ein Verfahren zur kryptographischen Bearbeitung mittels einer elliptischen Kurve, wobei mindestens ein Parameter der elliptischen Kurve verkürzt wird und somit eine Einsparung eines Teils des für die Parameter der elliptischen Kurve benötigten Speicherbereichs erfolgt;

Fig.2 eine Auswahl von Möglichkeiten für die Primzahl p, so daß der Parameter a der elliptischen Kurve verkürzt wird;

Fig.3 ein Verfahren zur Bestimmung einer elliptischen Kurve und anschließende Transformation in die zweite Form;

Fig.4 eine Anordnung zur kryptographischen Bearbeitung;

Fig.5 eine Prozessoreinheit.

Fig.1 zeigt ein Verfahren zur Bearbeitung mittels einer elliptischen Kurve. Die elliptische Kurve (vgl. Block 101) wird dazu von einer ersten Form in eine zweite Form transformiert (vgl. Block 102), ein Parameter der zweiten Form wird verkürzt (vgl. Block 103) und die zweite Form wird zur kryptographischen Bearbeitung abgespeichert (vgl. Block 104). Nachfolgend wird auf die genannten Schritte eingegangen, wobei einige Möglichkeiten für die Verkürzung beispielhaft herausgegriffen werden.

Es wird beschrieben, wie eine Reduzierung der Länge des Parameters a in der Gleichung der elliptischen Kurve (elliptische Kurve in erster Form, siehe Block 101)

$$y^2 = x^3 + ax + b \text{ über } GF(p) \qquad (3)$$

erreicht wird, wobei p insbesondere eine Primzahl größer 3 ist und GF(p) ein Galois-Feld mit p Elementen darstellt.

Eine elliptische Kurve

$$y^2 = x^3 + ax + b \text{ über } GF(p) \quad (4)$$

läßt sich durch Transformation in eine birational isomorphe elliptische Kurve (elliptische Kurve in zweiter Form, siehe Block 102)

$$y^2 = x^3 + c^4ax + c^6b \text{ über } GF(p) \quad (5)$$

überführen. Durch geeignete Wahl der Konstanten c kann der Koeffizient

$$c^4a \quad \text{bzw.} \quad (6)$$

$$-c^4a \quad (7)$$

verkürzt werden (siehe Block 103) mit dem Vorteil, daß der zur Speicherung dieses Koeffizienten benötigte Speicherplatz im Vergleich zum Speicherplatz für den Parameter a gering sein kann.

Entsprechend Gleichung (5) werden nachfolgend die Zahlen c^4a (bzw. $-c^4a$) und c^2 bestimmt.

1 Bestimmung der Zahl "c^4a"

Zur Bestimmung der Zahl c^4a (bzw. $-c^4a$) unterscheidet man bevorzugt die folgenden Fälle:

1.1 $p \equiv 3 \bmod 4$

In diesen Körpern gilt:

- alle Quadrate sind auch vierte Potenzen,

- '-1' ist kein Quadrat.

Es sei nun $p = 4k + 3$ und s eine vierte Potenz, welche die multiplikative Untergruppe der vierten Potenzen (bzw. der Quadrate) in GF(p) erzeugt.

Es ist

$V = \{1, s, s^2, s^3, \ldots, s^{2k}\}$ die Menge der vierten Potenzen in GF(p) und

$NQ = \{-1, -s, -s^2, -s^3, \ldots, -s^{2k}\}$ die Menge der Nichtquadrate in GF(p).

1. Zu jedem Element $a = s^t$ aus V existiert ein Element $c^4 = s^{2k+1-t}$ aus V mit $c^4 a = s^{2k+1} = 1$ in GF(p).
2. Zu jedem Element $a = -s^t$ aus V existiert ein Element $c^4 = s^{2k+1-t}$ aus V mit $c^4 a = -s^{2k+1} = -1$ in GF(p).

Dabei bezeichnen s, t und k Körperelemente aus GF(p).

Für $p \equiv 3 \bmod 4$ läßt sich der Parameter a durch geeignete Wahl der Konstanten c in die Zahl $c^4 a = 1$ in GF(p) oder $c^4 a = -1$ in GF(p) überführen.

1.2 $p \equiv 1 \bmod 4$

In einem solchen Körper gilt:

- (p-1)/4 Elemente der multiplikativen Gruppe des Körpers sind vierte Potenzen;
- (p-1)/4 Elemente der multiplikativen Gruppe des Körpers sind Quadrate, aber keine vierten Potenzen;
- (p-1)/2 Elemente der multiplikativen Gruppe des Körpers sind Nichtquadrate;

- '-1' ist kein Nichtquadrat.

A) $p \equiv 5 \bmod 8$

In einem solchen Körper gilt zusätzlich:
- '-1' ist ein Quadrat, aber keine vierte Potenz,
- '+2', '-2' sind Nichtquadrate.

Es sei nun $p = 8k + 5$ und s eine vierte Potenz, welche die multiplikative Untergruppe der vierten Potenz in GF(p) erzeugt.

Es ist

$V = \{1, s, s^2, s^3, \ldots, s^{2k}\}$ die Menge der vierten Potenzen in GF(p) und

$Q = \{-1, -s, -s^2, -s^3, \ldots, -s^{2k}\}$ die Menge der Quadrate, die keine vierten Potenzen in GF(p) sind und

$NQ = \{2, 2s, 2s^2, 2s^3, \ldots, 2s^{2k}, -2, -2s, -2s^2, -2s^3, \ldots, -2s^{2k}\}$ die Menge der Nichtquadrate in GF(p).

1. Zu jedem Element $a = s^t$ aus V existiert ein Element $c^4 = s^{2k+1-t}$ aus V mit $c^4 a = s^{2k+1} = 1$ in GF(p).
2. Zu jedem Element $a = -s^t$ aus Q existiert ein Element $c^4 = s^{2k+1-t}$ aus V mit $c^4 a = -s^{2k+1} = -1$ in GF(p).
3. Zu jedem Element $a = 2s^t$ aus NQ existiert ein Element $c^4 = s^{2k+1-t}$ aus V mit $c^4 a = 2s^{2k+1} = 2$ in GF(p).

4. Zu jedem Element existiert ein Element mit

$a = -2s^t$ aus NQ
$c^4 = s^{2k+1-t}$ aus V
$c^4a = -2s^{2k+1} = -2$ in GF(p).

Für $p \equiv 5 \bmod 8$ läßt sich der Parameter a durch geeignete Wahl der Konstanten c in die Zahl

$c^4a = 1$ oder -1 oder 2 oder -2 in GF(p)

überführen.

B) $p \equiv 1 \bmod 8$

Die Zahl c^4a läßt sich nach folgendem Schema ermitteln:

Für r=1,-1,2,-2,3,-3,4,-4,...
- bilde $z \equiv ra^{-1} \bmod p$;
- berechne $u \equiv z^{(p-1)/4} \bmod p$;
- abbrechen, falls u=1 ist;
- speichere $z = c^4$ und $r = c^4a$.

2 Bestimmung der Zahl "c^2 in GF(p)"

Zur Bestimmung der Zahl $c^2 \bmod p$ wird zunächst im entsprechenden Körper GF(p) festgestellt, ob a eine vierte Potenz, ein Quadrat aber keine vierte Potenz oder ein Nichtquadrat ist.

2.1 $p = 4k + 3$

In diesen Körpern wird $u = a^{(p-1)/2}$ in GF(p) berechnet.
- Ist u=1 in GF(p), so ist a eine vierte Potenz (bzw. ein Quadrat). In diesem Fall ist $c^4 = a^{-1}$ in GF(p).
- Ist u=-1 in GF(p), so ist a ein Nichtquadrat. In diesem Fall ist $c^4 = -a^{-1}$ in GF(p).

2.2 $p = 8k + 5$

In diesen Körpern wird $u = a^{(p-1)/4}$ in GF(p) berechnet.

- Ist u=1 in GF(p), so ist a eine vierte Potenz. In diesem Fall ist $c^4 = a^{-1}$ in GF(p).
- Ist u=-1, so ist a ein Quadrat aber keine vierte Potenz. In diesem Fall ist $c^4 = -a^{-1}$ in GF(p).
- Ist u weder 1 noch -1 in GF(p), so ist a ein Nichtquadrat in GF(p). In diesem Fall wird $v = (2a)^{(p-1)/4}$ in GF(p) berechnet. Ist v=1 in GF(p), so ist $c^4 = 2a^{-1}$ in GF(p), sonst ist $c^4 = -2a^{-1}$ in GF(p).

2.2 $p = 8k + 1$

In diesen Körpern ist nach dem in 1.2, Fall B beschriebenen Schema $z = c^4$.

In allen drei Fällen lassen sich mit einem Aufwand von O(log p) die beiden Wurzeln (c^2 und $-c^2$) aus c^4 berechnen. Für den Fall $p = 4k + 3$ ist nur eine der beiden angegebenen Lösungen zulässig, nämlich diejenige, die ein Quadrat in GF(p) ist. In den anderen Fällen sind beide Lösungen zulässig. Somit läßt sich der Koeffizient c^6b der elliptischen Kurve berechnen.

Aufgrund der geschlossenen Formeln für die Fälle $p = 4k + 3$ und $p = 8k + 5$ sind in der Praxis derartige Primzahlen zu bevorzugen.

Beispiel 1:

Es sei die Primzahl $p = 11 \Rightarrow$ Fall 1.1: $p \equiv 3 \bmod 4$

Zahl	Quadrate Q	vierte Potenzen V
1	1	1
2	4	5
3	9	4
4	5	3
5	3	9
6	3	9
7	5	3
8	9	4
9	4	5
10	1	1

Tabelle 1: Quadrate und vierte Potenzen mod 11

Damit ergeben sich die Menge der Quadrate Q, die Menge der vierten Potenzen V und die Menge der Nichtquadrate NQ zu:

$Q = V = \{1,3,4,5,9\}$;

$NQ = \{2,6,7,8,10\}$.

$a \in V = Q \quad \Rightarrow \quad ac^4 = 1$

a=	c^4=
1	1
3	4
4	3
5	9
9	5

Tabelle 2: Bestimmung von c^4 bei gegebenem Parameter a

$a \in NQ \quad \Rightarrow \quad ac^4 = -1$

a=	c^4=
2	5
6	9
7	3
8	4
10	1

Tabelle 3: Bestimmung von c^4 bei gegebenem Parameter a

Tabelle 2 zeigt verschiedene Möglichkeiten einer Wertzuordnung von a und c^4 auf, die in der Verknüpfung ac^4 stets 1 ergeben, und Tabelle 3 zeigt verschiedene Möglichkeiten einer Wertzuordnung von a und c^4 auf, die in der Verknüpfung ac^4 stets -1 ergeben. Dies gilt in GF(11).

Beispiel 2:

Es sei die Primzahl $p = 13 \Rightarrow$ Fall 1.2 A): $p \equiv 1 \bmod 4$ und zugleich $p \equiv 5 \bmod 8$.

Zahl	Quadrate Q	vierte Potenzen V
1	1	1
2	4	3
3	9	3
4	3	9
5	12	1
6	10	9
7	10	9
8	12	1
9	3	9
10	9	3
11	4	3
12	1	1

Tabelle 4: Quadrate und vierte Potenzen mod 13

Damit ergeben sich die Menge der Quadrate Q (die keine vierten Potenzen sind), die Menge der vierten Potenzen V und die Menge der Nichtquadrate NQ zu:

$Q = \{4,10,12\}$;

$V = \{1,3,9\}$;

$NQ = \{2,5,6,7,8,11\}$.

$a \in V \quad \Rightarrow \quad c^4 \in V$

a=	c^4=
1	1
3	9
9	3

Tabelle 5: Bestimmung von c^4 bei gegebenem Parameter a

$\Rightarrow ac^4 \equiv 1 \bmod 13$

$a \in Q$

a=	c^4 =	ac^4 =
4	3	12 = **-1** mod 13
10	9	90 = **-1** mod 13
12	1	12 = **-1** mod 13

Tabelle 6: Bestimmung von c^4 bei gegebenem Parameter a

$\Rightarrow ac^4 \equiv -1 \bmod 13$

$a \in NQ$

$NQ = \{2,5,6,7,8,11\}$, mit

$2*V = \{1,5,6\}$ und

$2*Q = \{7,8,11\}$

Fall a: $a \in NQ$ und $a \in (2 * V)$

a=	c^4 =	ac^4 =
2	1	2 = **2** mod 13
5	3	15 = **2** mod 13
6	9	54 = **2** mod 13

Tabelle 7: Bestimmung von c^4 bei gegebenem Parameter a

$\Rightarrow ac^4 \equiv 2 \bmod 13$

Fall b: $a \in NQ$ und $a \in (2 * Q)$

a=	c^4 =	ac^4 =
7	9	63 = **-2** mod 13
8	3	24 = **-2** mod 13
11	1	11 = **-2** mod 13

Tabelle 8: Bestimmung von c^4 bei gegebenem Parameter a

$\Rightarrow ac^4 \equiv -2 \bmod 13$

Die auf die beschriebene Art gewonnene elliptische Kurve in der zweiten Form (siehe Block 103) wird zu einer kryptographischen Bearbeitung eingesetzt.

Fig.2 zeigt eine Auswahl von Möglichkeiten für die Wahl der Primzahl p zur Verkürzung des Parameters a (siehe Block 201), wie oben beschrieben. Die Möglichkeit 202 bestimmt p derart, daß $p = 3 \bmod 4$ gilt. In diesem Fall läßt sich der Parameter a anhand oben beschriebener Vorgehensweise verkürzen. Das gleiche gilt für $p = 1 \bmod 4$ (Fall 203), wobei eine Fallunterscheidung gesondert die beiden Fälle $p = 5 \bmod 8$ (Fall 204) und $p = 1 \bmod 8$ (Fall 205) anführt. Die geschlossenen Formulierungen zur Bestimmung eines verkürzten Parameters a sind jeweils oben ausgeführt. Fig.2 zeigt ausdrücklich eine Auswahl von Möglichkeiten auf, ohne einen Anspruch auf eine umfassende Auswahl anzustreben.

In **Fig.3** wird in einem ersten Schritt 301 eine elliptische Kurve mit den Parametern a, b, p und einer Punktezahl ZP gemäß Gleichung (1) bestimmt. In einem Schritt 302 wird die elliptische Kurve transformiert (vgl. Gleichung (2)). Nach der Transformation umfaßt die elliptische Kurve die Parameter a', b', p und ZP. a' und b' deuten an, daß die Parameter a und b verändert wurden, wobei ein Parameter, vorzugsweise der Parameter a' kurz ist im Vergleich zu dem Parameter a, so daß durch Abspeichern des Parameters a' anstelle des Parameters a als Kennzeichen der elliptischen Kurve Speicherplatz eingespart wird.

In **Fig.4** ist eine Anordnung zur kryptographischen Bearbeitung dargestellt.

Ein portables Medium 401, vorzugsweise eine Chipkarte, umfaßt einen (unsicheren) Speicherbereich MEM 403 und einen geschützten (sicheren) Speicherbereich SEC 402. Anhand einer Schnittstelle IFC 404 werden über einen Kanal 405 Daten zwischen dem Medium 401 und einem Rechnernetz 406 ausgetauscht. Das Rechnernetz 406 umfaßt mehrere Rechner, die miteinander verbunden sind und untereinander kommunizieren. Daten für den Betrieb des portablen Mediums 401 sind vorzugsweise in dem Rechnernetz RN 406 verteilt verfügbar.

Der geschützte Speicherbereich 402 ist nicht lesbar ausgeführt. Anhand einer Recheneinheit, die auf dem portablen Medium 401 oder im Rechnernetz 406 untergebracht ist, werden die Daten des geschützte Speicherbereichs 402 genutzt. So kann eine Vergleichsoperation als Ergebnis angeben, ob ein Vergleich einer Eingabe mit einem Schlüssel im geschützte Speicherbereich 402 erfolgreich war oder nicht.

Die Parameter der elliptischen Kurve sind in dem geschützten Speicherbereich 402 oder in dem ungeschützten Speicherbereich 403 abgelegt. Insbesondere wird ein geheimer oder privater

Schlüssel in dem geschützten Speicherbereich und ein öffentlicher Schlüssel in dem unsicheren Speicherbereich abgespeichert.

In **Fig.5** ist eine Recheneinheit 501 dargestellt. Die Recheneinheit 501 umfaßt einen Prozessor CPU 502, einen Speicher 503 und eine Input/Output-Schnittstelle 504, die über ein aus der Recheneinheit 501 herausgeführtes Interface 505 auf unterschiedliche Art und Weise genutzt wird: Über eine Grafikschnittstelle wird eine Ausgabe auf einem Monitor 507 sichtbar und/oder auf einem Drucker 508 ausgegeben. Eine Eingabe erfolgt über eine Maus 509 oder eine Tastatur 510. Auch verfügt die Recheneinheit 501 über einen Bus 506, der die Verbindung von Speicher 503, Prozessor 502 und Input/Output-Schnittstelle 504 sicherstellt. Weiterhin ist es möglich, an den Bus 506 zusätzliche Komponenten anzuschließen: zusätzlicher Speicher, Festplatte, etc.

Literaturverzeichnis:

[1] Neal Koblitz: A Course in Number Theory and Cryptography, Springer Verlag New York, 1987, ISBN 0-387-96576-9, Seiten 150-179.

[2] Alfred J. Menezes: Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, Massachusetts 1993, ISBN 0-7923-9368-6, Seiten 83-116.

[3] Rudolf Lidl, Harald Niederreiter: Introduction to finite fields and their applications, Cambridge University Press, Cambridge 1986, ISBN 0-521-30706-6, Seiten 15, 45.

[4] Christoph Ruland: Informationssicherheit in Datennetzen, DATACOM-Verlang, Bergheim 1993, ISBN 3-89238-081-3, Seiten 73-85.

Patentansprüche

1. Verfahren zur kryptographischen Bearbeitung anhand einer elliptischen Kurve auf einem Rechner,
   a) bei dem die elliptische Kurve in einer ersten Form vorgegeben wird, wobei mehrere erste Parameter die elliptische Kurve bestimmen,
   b) bei dem die elliptische Kurve in eine zweite Form transformiert wird, indem mehrere zweite Parameter bestimmt werden, wobei mindestens einer der zweiten Parameter in seiner Länge gegenüber dem ersten Parameter verkürzt wird.
   c) bei dem die elliptische Kurve in der zweiten Form zur kryptographischen Bearbeitung bestimmt wird.

2. Verfahren nach dem vorhergehenden Anspruch, bei dem die erste Form der elliptischen Kurve bestimmt ist durch

$$y^2 = x^3 + ax + b,$$

wobei
x,y Variablen und
a,b die ersten Parameter
bezeichnen.

3. Verfahren nach Anspruch 1 oder 2, bei dem die zweite Form der elliptischen Kurve bestimmt ist durch

$$y^2 = x^3 + c^4ax + c^6b,$$

wobei
x,y Variablen,
a,b die ersten Parameter und
c eine Konstante
bezeichnen.

4. Verfahren nach einem der Ansprüche 1 bis 3, bei dem der Parameter a verkürzt wird, indem die Konstante c derart gewählt wird, daß

$$c^4 a \bmod p$$

deutlich kürzer bestimmt wird als die Längen des Parameters b und die Länge der vorgegebenen Größe p.

5. Verfahren nach einem der vorhergehenden Ansprüche, bei dem eine kryptographische Verschlüsselung durchgeführt wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, bei dem eine kryptographische Entschlüsselung durchgeführt wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, bei dem eine Schlüsselvergabe durchgeführt wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, bei dem eine digitale Signatur durchgeführt wird.

9. Verfahren nach Anspruch 8, bei dem eine Verifikation der digitalen Signatur durchgeführt wird.

10. Verfahren nach einem der vorhergehenden Ansprüche, bei dem eine asymmetrische Authentikation durchgeführt wird.

11. Vorrichtung zur kryptographischen Bearbeitung, mit einer Prozessoreinheit, die derart eingerichtet ist, daß

a) eine elliptische Kurve in einer ersten Form vorgegeben wird, wobei mehrere erste Parameter die elliptische Kurve bestimmen,

b) die elliptische Kurve in eine zweite Form transformiert wird, indem mehrere zweite Parameter bestimmt werden, wobei mindestens einer der zweiten Parameter in seiner Länge gegenüber den ersten Parameter verkürzt wird.

c) die elliptische Kurve in der zweiten Form zur kryptographischen Bearbeitung bestimmt wird.

12. Vorrichtung nach Anspruch 11,
bei der die Prozessoreinheit derart eingerichtet ist, daß die erste Form der elliptischen Kurve bestimmt ist durch

$$y^2 = x^3 + ax + b,$$

wobei

x,y Variablen und
a,b die ersten Parameter

bezeichnen.

13. Vorrichtung nach Anspruch 11 oder 12,
bei der die Prozessoreinheit derart eingerichtet ist, daß die zweite Form der elliptischen Kurve bestimmt ist durch

$$y^2 = x^3 + c^4ax + c^6b,$$

wobei

x,y Variablen,
a,b die ersten Parameter und
c eine Konstante

bezeichnen.

14. Vorrichtung nach einem der Ansprüche 11 bis 13,
bei der die Prozessoreinheit derart eingerichtet ist, daß

der Parameter a verkürzt wird, indem die Konstante c derart gewählt wird, daß

$$c^4 a \bmod p$$

deutlich kürzer bestimmt wird als die Längen des Parameters b und die Länge der vorgegebenen Größe p.

15. Vorrichtung nach einem der Ansprüche 11 bis 14, bei der die Vorrichtung eine Chipkarte mit einem Speicherbereich ist, wobei in dem Speicherbereich die Parameter der elliptischen Kurve abspeicherbar sind..

16. Vorrichtung nach Anspruch 15, bei dem ein geheimer Schlüssel in einem geschützten Speicherbereich der Chipkarte abspeicherbar ist.

FIG 1

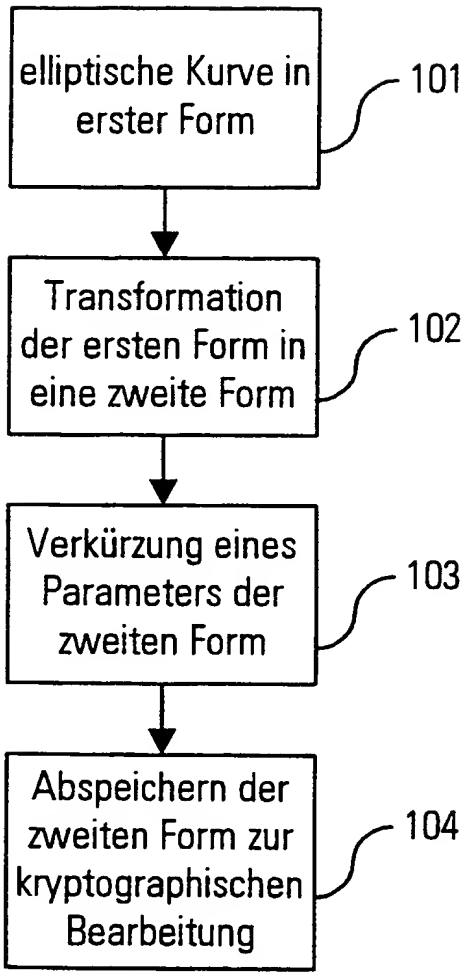


FIG 2

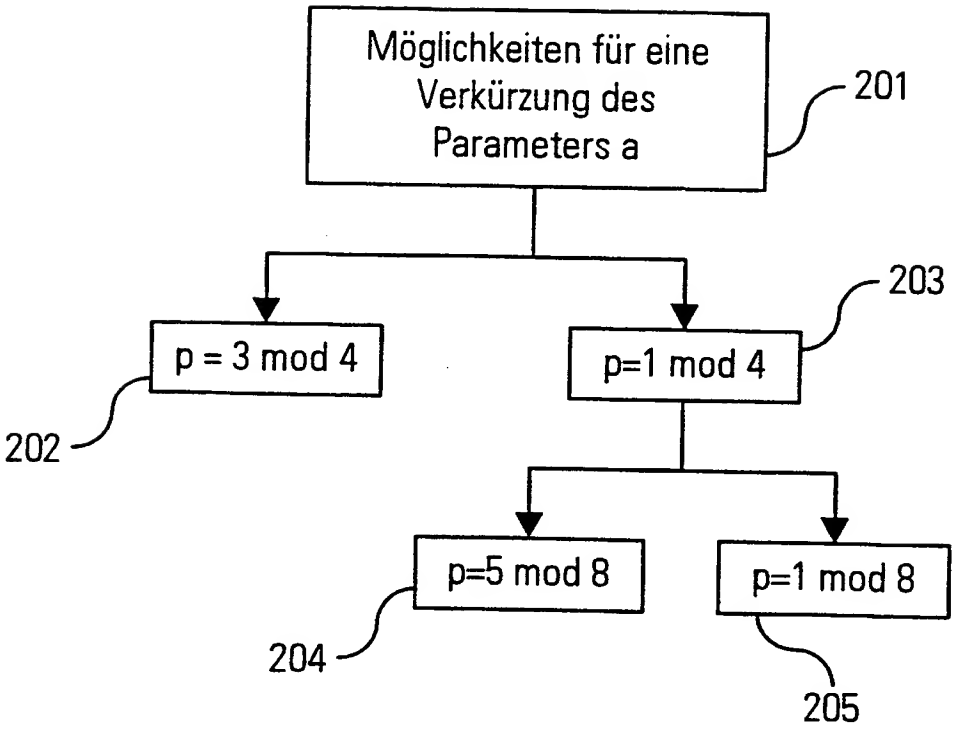


FIG 3

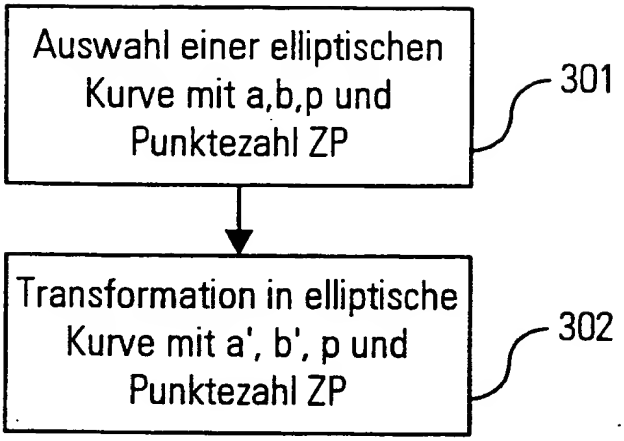

Auswahl einer elliptischen Kurve mit a,b,p und Punktezahl ZP
301
Transformation in elliptische Kurve mit a', b', p und Punktezahl ZP
302

FIG 4

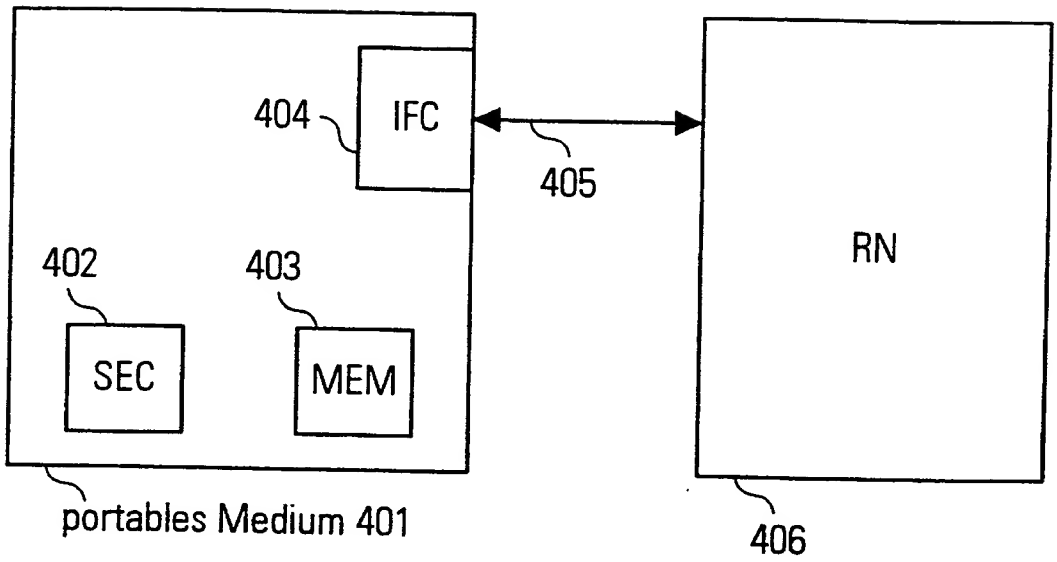
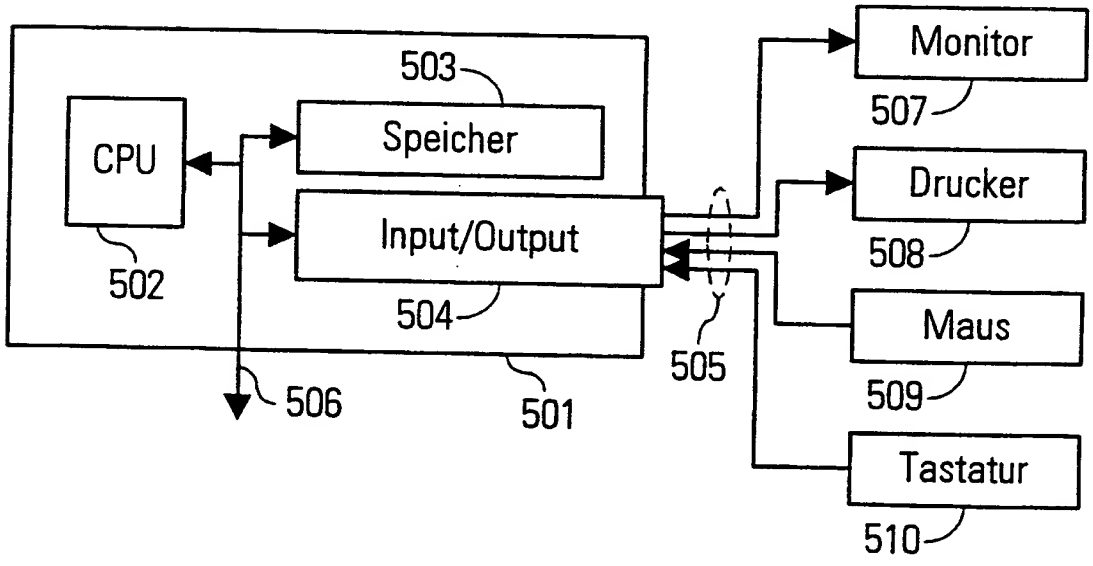


FIG 5



INTERNATIONAL SEARCH REPORT

Int ...tional Application No
PCT/DE 99/00278

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 497 423 A (MIYAJI ATSUKO) 5 March 1996 (1996-03-05) abstract column 6, line 31 - line 67 column 7, line 5 - line 22 claim 1 figures 1,5 ---	1,2,5,6, 8,9,11, 12
A	US 5 442 707 A (MIYAJI ATSUKO ET AL) 15 August 1995 (1995-08-15) abstract column 8, line 8 - line 53 column 18, line 29 - column 19, line 33 figure 3 --- -/--	1,2,5,6, 8,9, 11-16

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 July 1999	19/07/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int. tional Application No
PCT/DE 99/00278

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	MIYAJI A: "ELLIPTIC CURVES SUITABLE FOR CRYPTOSYSTEMS" IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, vol. E77-A, no. 1, 1 January 1994 (1994-01-01), pages 98-104, XP000439669 ISSN: 0916-8508 the whole document	1,11

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. tional Application No
PCT/DE 99/00278

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5497423 A	05-03-1996	JP 7098563 A	11-04-1995
US 5442707 A	15-08-1995	JP 6110386 A	22-04-1994
		JP 6295154 A	21-10-1994

INTERNATIONALER RECHERCHENBERICHT

Int ...tionales Aktenzeichen
PCT/DE 99/00278

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/30

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 5 497 423 A (MIYAJI ATSUKO) 5. März 1996 (1996-03-05) Zusammenfassung Spalte 6, Zeile 31 - Zeile 67 Spalte 7, Zeile 5 - Zeile 22 Anspruch 1 Abbildungen 1,5 ---	1,2,5,6, 8,9,11, 12
A	US 5 442 707 A (MIYAJI ATSUKO ET AL) 15. August 1995 (1995-08-15) Zusammenfassung Spalte 8, Zeile 8 - Zeile 53 Spalte 18, Zeile 29 - Spalte 19, Zeile 33 Abbildung 3 --- -/--	1,2,5,6, 8,9, 11-16

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
12. Juli 1999	19/07/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 99/00278

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	MIYAJI A: "ELLIPTIC CURVES SUITABLE FOR CRYPTOSYSTEMS" IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, Bd. E77-A, Nr. 1, 1. Januar 1994 (1994-01-01), Seiten 98-104, XP000439669 ISSN: 0916-8508 das ganze Dokument	1,11

1

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE 99/00278

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5497423 A	05-03-1996	JP 7098563 A	11-04-1995
US 5442707 A	15-08-1995	JP 6110386 A	22-04-1994
		JP 6295154 A	21-10-1994